MORGAN & MORGAN
Michael F. Ram (SBN 104805)
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Tel: (415) 358-6913
mram@forthepeople.com

MORGAN & MORGAN
John A. Yanchunis (*pro hac vice* forthcoming)
Ryan J. McGee (*pro hac vice* forthcoming)
Ronald Podolny (*pro hac vice* forthcoming)
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel: (813) 223-5505
jyanchunis@forthepeople.com
rmcgee@forthepeople.com
ronald.podolny@forthepeople.com

Counsel of Plaintiffs and the proposed class

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA

SHANDRELLE OKONI, individually and on behalf of A. H-M. 1, L.M., and A. H-M 2, minors, and on behalf of all others similarly situated,

Plaintiffs,

v.

POWERSCHOOL GROUP, LLC, and POWERSCHOOL HOLDINGS, INC.,

Defendants.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMAND

Plaintiff Shandrelle Okoni ("Plaintiff"), individually, and on behalf of A. H-M. 1, L. M., and A. H-M 2, minors, and on behalf of all others similarly situated, brings this action against PowerSchool Group, LLC and PowerSchool Holdings Inc. (collectively, "PowerSchool" or "Defendant"). The following allegations are based on Plaintiff's knowledge, investigations of counsel, facts of public record, and information and belief.

NATURE OF THE ACTION

1. Plaintiff seeks to hold the Defendant responsible for the injuries the Defendant inflicted on Plaintiff and her minor children, and tens of millions of similarly situated persons ("Class Members") due to the Defendant's impermissibly inadequate and unlawful data security, which caused the personal information of Plaintiff and those similarly situated to be exfiltrated by unauthorized access by cybercriminals (the "Data Breach") on or about December 28, 2024.

2. Defendant is a provider of cloud-based software to K-12 educational institutions in North America.[1]

3. The Data Breach affected some 60 million teachers and students whose data was kept in cloud software solutions provided by Defendant.[2] The data which the Defendant collected from the Plaintiff and Class Members, and which was exfiltrated by cybercriminals from the Defendant, were highly sensitive. The exfiltrated data included personal identifying information ("PII") and personal health information ("PHI" and, together with Personal Information, "Personal Information") including, but not limited to, names and social security numbers, medical information and grade information.[3]

4. Prior to and through the date of the Data Breach, the Defendant obtained Plaintiff's and Class Members' Personal Information and then maintained that sensitive data in a negligent

[1] "About". PowerSchool, https://www.powerschool.com/company/ (last accessed on January 15, 2025).
[2] Adam Marshall, "60 Million Students and teachers Targeted in PowerSchool Data Breach", Tech.Co (January 14, 2025), https://tech.co/news/powerschool-data-breach (last accessed on January 16, 2025); Carly Page, "PowerSchool data breach victims say hackers stole 'all' historical student and teacher data." (January 15, 2025), https://techcrunch.com/2025/01/15/powerschool-data-breach-victims-say-hackers-stole-all-historical-student-and-teacher-data/ (last accessed on January 15, 2025).
[3] PowerSchool, https://www.powerschool.com/security/sis-incident/ (last accessed on January 16, 2025).

and/or reckless manner. As evidenced by the Data Breach, the Defendant inadequately and unlawfully maintained its network, platform, software—rendering these easy prey for cybercriminals.

5. The risk of the Data Breach was known to the Defendant. Thus, the Defendant was on notice that its inadequate data security created a heightened risk of exfiltration, compromise, and theft.

6. Then, after the Data Breach, Defendant failed to provide timely notice to the affected Plaintiff and Class Members, thereby exacerbating their injuries. Ultimately, Defendant deprived Plaintiff and Class Members of the chance to take speedy measures to protect themselves and mitigate harm. Simply put, Defendant impermissibly left Plaintiff and Class Members in the dark—thereby causing their injuries to fester and the damage to spread.

7. Even when Defendant finally notified Plaintiff and Class Members of their Personal Information exfiltration, Defendant failed to adequately describe the Data Breach and its effects, as well as the measures it took to prevent data breaches from occurring in the future.

8. Today, the identities of Plaintiff and Class Members are in jeopardy—all because of Defendant's negligence. Plaintiff and Class Members now suffer from a present and continuing risk of fraud and identity theft and must now constantly monitor their financial accounts.

9. Armed with the PII and PHI stolen in the Data Breach, criminals can commit a boundless litany of financial crimes. Specifically, and without limitation, criminals can now open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

10. Plaintiff and Class Members will likely suffer additional financial costs for purchasing necessary credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

11. Plaintiff and Class Members have suffered—and will continue to suffer—from the loss of the benefit of their bargain, unexpected out-of-pocket expenses, lost or diminished value of their Personal Information, emotional distress, and the value of their time reasonably incurred to mitigate the fallout of the Data Breach.

12. Through this action, Plaintiff seeks to remedy these injuries on behalf of themselves and all similarly situated individuals whose Personal Information was exfiltrated and compromised in the Data Breach.

13. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief—including improvements to Defendant's data security systems, future annual audits, and the appointment of an independent and qualified cyber auditor to monitor Defendant's cyber hygiene, all of which will be funded by Defendant.

PARTIES

14. Plaintiff Okoni is a natural person and resident and citizen of North Charleston, South Carolina. Okoni brings this suit in her personal capacity and on behalf of her three minor children: A. H-M. 1, L. M., and A. H-M 2.

15. On or about January 9, 2025, Okoni received an email from her children's school district, informing her of a "cybersecurity incident involving PowerSchool," which served as the student information system provider used by our district" ("Data Breach Notification"), as described more fully below. She received a further update on January 10, 2025 regarding the same Data Breach.

16. Defendant PowerSchool Group LLC is a Delaware limited liability company, with its headquarters located at: 150 Parkshore Dr., Folsom, CA 95630.

17. Defendant PowerSchool Holdings, Inc. is a Delaware corporation, with its headquarters located at: 150 Parkshore Dr., Folsom, CA 95630.

18. Together, PowerSchool Group LLC and PowerSchool Holdings, Inc. operate a cloud-based software company which held Plaintiffs' Personal Information and suffered the Data Breach described herein.

JURISDICTION AND VENUE

19. This Court has original subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Minimal diversity is established because many members of the class are citizens of states different than that of Defendant.

20. This Court has personal jurisdiction over Defendant, because Defendant maintains its principal place of business in this district.

21. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant maintains its principal place of business in the jurisdiction.

FACTUAL ALLEGATIONS

Defendant Collected and Stored the Personal Information of Plaintiff and Class Members

22. Defendant provides cloud-based software solutions to school districts throughout North America.

23. Defendant received and maintained the Personal Information of its clients', students and teachers, such as individuals' including, but not limited to, names and social security numbers, medical information and grade information. These records were, and continue to be, stored on Defendant's computer systems.

24. Because of the highly sensitive and personal nature of the information Defendant acquires and stores, Defendant knew or reasonably should have known that it stored protected Personal Information and must comply with industry standards related to data security and all federal and state laws protecting customers' Personal Information and provide adequate notice to customers if their Personal Information is disclosed without proper authorization.

25. When Defendant collects this sensitive information, it promises to use reasonable measures to safeguard the Personal Information from theft and misuse.

26. By obtaining, collecting, receiving, and/or storing Plaintiff's and Class Members' Personal Information, Defendant assumed legal and equitable duties and knew, or should have

known, that they were thereafter responsible for protecting Plaintiff's and Class Members' Personal Information from unauthorized disclosure.

27. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Personal Information, including but not limited to, protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

28. Plaintiff and Class Members relied on Defendant to keep their Personal Information confidential and securely maintained, to use this information for education purposes only, and to make only authorized disclosures of this information.

29. Defendant could have prevented or mitigated the effects of the Data Breach by better securing its network, properly encrypting its data, or better selecting its information technology partners.

30. Defendant's negligence in safeguarding Plaintiff's and Class Members' Personal Information was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

31. Despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' Personal Information from being compromised.

32. Defendant failed to properly select its information security partners.

33. Defendant failed to ensure fair, reasonable, or adequate computer systems and data security practices to safeguard the Personal Information of Plaintiff and Class Members.

34. Defendant failed to timely and accurately disclose that Plaintiff's and Class Members' Personal Information had been improperly acquired or accessed.

35. Upon information and belief, Defendant failed to ensure the proper implementation of sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.

36. Upon information and belief, Defendant failed to ensure the proper encryption of Plaintiff's and Class Members' Personal Information and monitor user behavior and activity to identify possible threats.

The Data Breach

37. On or about January 6, 2025, Plaintiff received an email from her children's school district, informing her of "Student Account Lockouts", which stated, in relevant part:

> We wanted to inform you about an issue that occurred over the weekend, which resulted in a significant number of student accounts being temporarily locked.
>
> CCSD's IT team is actively working alongside the Tech Liaisons at schools to resolve the matter and restore account access for affected students as quickly as possible.
>
> We apologize for any inconvenience this may have caused and appreciate your patience
> and understanding as we work to address the situation.

38. On or about January 9, 2025, Plaintiff received a further email from her children's school district, notifying her of the Data Berach, which stated, in relevant part:

> The SC Department of Education (SCDE) has reported a cybersecurity breach involving PowerSchool. Personally identifiable information (PII) from PowerSchool's systems was compromised, impacting multiple states and school districts, including ours.
>
> PowerSchool has stated the breach is contained and has taken steps to secure its systems. SCDE is working with PowerSchool, law enforcement, and districts to assess the impact and provide guidance.
>
> Please know that the privacy and safety of our students and staff remain our top priority. As more information becomes available, we will share updates with you.

39. The email did not promise any assistance on the part of Defendant.

40. On or about January 10, 2025, Plaintiff received a further email from her children's school district, which stated, in the relevant part:

> Yesterday, we informed you of a cybersecurity incident involving PowerSchool, the student information system provider used by our district.
>
> **Key Points for Your Awareness:**

> - **Investigation Underway:** SCDE, SLED, and other state and federal agencies are actively investigating this incident.
> - **Source of Breach:** The breach occurred through a compromised customer support credential belonging to PowerSchool.
> - **PowerSchool's Response:** PowerSchool has taken full responsibility for the breach and has implemented measures to contain and mitigate the incident.
>
> The SCDE has issued an official release with additional information, which you can access here.
>
> We are committed to keeping our students, families, and staff informed and will continue to provide updates as they become available.

41. It is likely the Data Breach was targeted at the Defendant due to its status as a an organization that collects, creates, and maintains Personal Information.

42. Defendant was untimely and unreasonably delayed in providing notice of the Data Breach to Plaintiff and Class Members.

43. Time is of the essence when highly sensitive Personal Information is subject to unauthorized access and/or acquisition.

44. The disclosed, accessed, and/or acquired Personal Information of Plaintiff and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted Personal Information to criminals. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their Personal Information onto the Dark Web. Plaintiff and Class Members, including many minors, now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing sensitive personal information.

45. In sum, Defendant largely put the burden on Plaintiff and Class Members to take measures to protect themselves.

46. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[4]

47. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[5] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[6] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

48. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

49. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' Personal Information with the intent of engaging in misuse of the Personal Information, including marketing and selling Plaintiff's and Class Members' Personal Information.

50. Defendant has offered no measures to protect Plaintiff and Class Members from the lifetime risks they each now face. As another element of damages, Plaintiff and Class Members

[4] *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=%20In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last accessed April 25, 2024); *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data*, *https://www.bls.gov/news.release/pdf/wkyeng.pdf* (last accessed April 25, 2024) (finding that on average, private-sector workers make $1,145 per 40-hour work week.).

[5] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (Nov. 6, 2019) (last accessed April 25, 2024).

[6] *Id.*

seek a sum of money sufficient to provide Plaintiff and Class Members identity theft protection services for a lifetime.

51. Defendant had and continues to have obligations created by reasonable industry standards, common law, state statutory law, and its own assurances and representations to keep Plaintiff's and Class Members' Personal Information confidential and to protect such Personal Information from unauthorized access.

52. Plaintiff and the Class Members remain, even today, in the dark regarding the scope of the data breach, what particular data was stolen, beyond several categories listed in the letter as "included" in the Data Breach, and what steps are being taken, if any, to secure their Personal Information going forward. Plaintiff and Class Members are left to speculate as to the full impact of the Data Breach and how exactly the Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

53. Plaintiff's and Class Members' Personal Information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed Personal Information for targeted marketing without the approval of Plaintiff and/or Class Members. Either way, unauthorized individuals can now easily access the Personal Information and/or financial information of Plaintiff and Class Members.

Defendant Failed to Comply with FTC Guidelines

54. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[7] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exfiltration of Personal Information.

55. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[8] The guidelines explain that businesses should:

[7] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://bit.ly/3uSoYWF (last accessed April 25, 2024).

[8] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://bit.ly/3u9mzre (last accessed April 25, 2024).

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

56. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

57. The FTC recommends that companies not maintain Personal Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[9]

58. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

59. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Personal Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

60. Despite its alleged commitments to securing sensitive data, Defendant does not follow industry standard practices in securing Personal Information.

61. Experts studying cyber security routinely identify financial service providers as being particularly vulnerable to cyberattacks because of the value of the Personal Information

[9] *See Start With Security, A Guide for Business*, FED. TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited March 16, 2024).

which they collect and maintain.

62. Several best practices have been identified that at a minimum should be implemented by financial service providers like Defendant, including but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

63. Other best cybersecurity practices that are standard in the financial service industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

64. Such frameworks are the existing and applicable industry standards in the financial service industry. Defendant failed to comply with these accepted standards, thus opening the door to criminals and the Data Breach.

The Experiences and Injuries of Plaintiff and Class Members

65. Plaintiff and Class Members are current and former students and teachers of Defendant's clients (school boards or individual schools). As a condition of studying or working at its clients', the Defendant required Plaintiff and Class Members to disclose their Personal Information.

66. Plaintiff suffered actual injury and damages as a result of the Data Breach. Plaintiff would not have provided Defendant with her Personal Information had Defendant disclosed that it lacked security practices adequate to safeguard PII and PHI.

67. Plaintiff suffered actual injury in the form of damages and diminution in the value of her Personal Information – a form of intangible property that she entrusted to Defendant.

68. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increase concerns for the loss of her privacy, especially her and her children's PHI.

69. Plaintiff reasonably believes that her, and her children's, Personal Information may have already been sold to by the cybercriminals. Had she been notified of Defendant's Data Breach by Defendant itself, in a more timely manner, she could have attempted to mitigate her injuries.

70. Plaintiff has suffered present and continuing injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her, and her children's, stolen Personal Information being placed in the hands of unauthorized third parties and possibly criminals.

71. Plaintiff has a continuing interest in ensuring that her and her children's Personal Information, which upon information and belief remains backed up and in Defendant's possession, is protected and safeguarded from future breaches.

72. Notably, Defendant did not provide notice to Plaintiff. Plaintiff received notice from her children's school board.

73. Because of the Data Breach, Defendant inflicted injuries upon Plaintiff and Class Members. And yet, Defendant has done little to provide Plaintiff and the Class Members with relief for the damages they suffered.

74. All Class Members were injured when Defendant caused their Personal Information to be exfiltrated by cybercriminals.

75. Plaintiff and Class Members entrusted their Personal Information to Defendant. Thus, Plaintiff had the reasonable expectation and understanding that Defendant would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify them of any data security incidents. Plaintiff and Class Members would not have entrusted their Personal Information to Defendant had they known that Defendant would not take reasonable steps to safeguard their information.

76. Plaintiff and Class Members suffered actual injury from having their Personal Information compromised in the Data Breach including, but not limited to, (a) damage to and diminution in the value of their Personal Information—a form of property that Defendant obtained from Plaintiff; (b) violation of their privacy rights; (c) the likely theft of their Personal Information;

(d) fraudulent activity resulting from the Data Breach; and (e) present and continuing injury arising from the increased risk of additional identity theft and fraud.

77. As a result of the Data Breach, Plaintiff and Class Members also suffered emotional distress because of the release of their Personal Information—which they believed would be protected from unauthorized access and disclosure. Now, Plaintiff and Class Members suffer from anxiety about unauthorized parties viewing, selling, and/or using their Personal Information for nefarious purposes like identity theft and fraud.

78. Plaintiff and Class Members also suffer anxiety about unauthorized parties viewing, using, and/or publishing their information related to their medical records and prescriptions.

79. Because of the Data Breach, Plaintiff and Class Members have spent—and will continue to spend—considerable time and money to try to mitigate and address harms caused by the Data Breach.

Plaintiff and the Proposed Class Face Significant Risk of Present and Continuing Identity Theft

80. Plaintiff and Class Members suffered injury from the misuse of their Personal Information that can be directly traced to Defendant.

81. The ramifications of Defendant's failure to keep Plaintiff's and the Class's Personal Information secure are severe. Identity theft occurs when someone uses another's personal such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

82. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[10]

83. As a result of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiff and Class Members suffered and will continue to suffer damages, including

[10]Anne Saita, "Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims", Threat Post, (Feb. 20, 2013) https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/ (last visited on May 14, 2024).

monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Personal Information is used;

b. The diminution in value of their Personal Information;

c. The compromise and continuing publication of their Personal Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Personal Information; and

h. The continued risk to their Personal Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Personal Information in their possession.

84. Stolen Personal Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen Personal Information can be worth up to $1,000.00 depending on the type of information obtained.[11]

85. The value of Plaintiff's and the proposed Class's Personal Information on the black market is considerable. Stolen Personal Information trades on the black market for years, and

[11] Brian Stack, "Here's How Much Your Personal Information Is Selling for on the Dark Web," EXPERIAN (Dec. 6, 2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on May 14, 2024).

criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

86. It can take victims years to spot or identify Personal Information theft, giving criminals plenty of time to milk that information for cash.

87. One such example of criminals using Personal Information for profit is the development of "Fullz" packages.[12]

88. Cyber-criminals can cross-reference two sources of Personal Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

89. The development of "Fullz" packages means that stolen Personal Information from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Personal Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen Personal Information is being misused, and that such misuse is fairly traceable to the Data Breach.

[12] "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, "Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm," KREBS ON SECURITY, (Sep. 18, 2014) https://krebsonsecurity.com/tag/fullz/ (last visited on May 14, 2024).

90. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

91. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiff and the Class that their Personal Information had been stolen.

92. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

93. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their Personal Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

94. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Personal Information. To protect themselves, Plaintiff and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

95. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[13]

[13] "Commissioner Pamela Jones Harbour: Remarks Before FTC Exploring Privacy Roundtable," FED. TRADE COMMISSION (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited on May 14, 2024).

CLASS ACTION ALLEGATIONS

96. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class") under Fed. R. Civ. P. 23(b)(2), 23(b)(3), and 23(c)(4).

97. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons residing in the United States whose Personal Information was impacted by the Data Breach at PowerSchool Holdings, Inc. and its affiliated entities, which occurred on or about December 28, 2024.

98. The Class defined above is readily ascertainable from information in Defendant's possession. Thus, such identification of Class Members will be reliable and administratively feasible.

99. Excluded from the Class are: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent has a controlling interest, and these entities' current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

100. Plaintiff reserves the right to amend or modify the Class definition—including potential Subclasses—as this case progresses.

101. Plaintiff and Class Members satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

102. **Numerosity**. The Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of tens of thousands of individuals who reside in the U.S. and were or are students or teachers at Defendant's clients, and whose Personal Information was compromised by the Data Breach.

103. **Commonality**. There are many questions of law and fact common to the Class. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

a. If Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Personal Information;

b. If Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. If Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. If Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. If Defendant owed a duty to Class Members to safeguard their Personal Information;

f. If Defendant breached its duty to Class Members to safeguard their Personal Information;

g. If Defendant failed to comply with the HIPAA Security Rule (45 CFR 160 and Subparts A and C of Part 164) by failing to implement reasonable security procedures and practices to protect the integrity and availability of PHI;

h. If Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. If Defendant should have discovered the Data Breach earlier;

j. If Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

k. If Defendant failed to provide notice of the Data Breach in a timely manner;

l. If Defendant's delay in informing Plaintiff and Class Members of the Data Breach was unreasonable;

m. If Defendant's method of informing Plaintiff and Class Members of the Data Breach was unreasonable;

n. If Defendant's conduct was negligent;

o. If Plaintiff and Class Members were injured as a proximate cause or result of the Data Breach;

p. If Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

q. If Defendant breached implied contracts with Plaintiff and Class Members;

r. If Defendant was unjustly enriched as a result of the Data Breach; and

s. If Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

104. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach. Moreover, all Plaintiff and Class Members were subjected to Defendant's uniformly illegal and impermissible conduct.

105. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating complex class actions. Plaintiff has no interests that conflict with, or are antagonistic to, those of the Class.

106. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff and Class Members' data was stored on the same network system and unlawfully and inadequately protected in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

107. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class

Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

108. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

109. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

110. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above, including in paragraph 103.

111. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

112. Plaintiff re-alleges and incorporates by reference paragraphs 1-111 of the Complaint as if fully set forth herein.

113. Defendant required Plaintiff's and Class Members' to submit non-public Personal Information to Defendant to receive Defendant's clients' education services, or to obtain employment from Defendant's clients.

114. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer system—and Plaintiff's and Class Members' Personal Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes so it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

115. The risk that unauthorized persons would attempt to gain access to the Personal Information and misuse it was foreseeable to Defendant. Given that Defendant holds vast amounts of Personal Information, it was inevitable that unauthorized individuals would at some point try to access Defendant's databases of Personal Information.

116. After all, Personal Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Personal Information of Plaintiff and Class Members. Thus, Defendant knew, or should have known, the importance of exercising reasonable care in handling the Personal Information entrusted to them.

117. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its, or its service providers', systems and networks, and the personnel responsible for them, adequately protected the Personal Information.

118. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and Class Members, which is recognized by laws and regulations, as well as common law. Defendant was in a superior position to ensure that its own, and its service providers', systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

119. Defendant failed to take appropriate measures to protect the Personal Information of Plaintiff and the Class. Defendant is morally culpable, given the prominence of security breaches in the financial services industry, including the insurance industry. Any purported safeguards that Defendant had in place were wholly inadequate.

120. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' Personal Information by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite known data breaches in the financial service industry, and allowing unauthorized access to Plaintiff's and the other Class Members' Personal Information.

121. The Defendant was negligent in failing to comply with industry and federal regulations in respect of safeguarding and protecting Plaintiff's and Class Members' Personal Information.

122. But for Defendant's wrongful and negligent breach of its duties to Plaintiff and the Class, Plaintiff's and Class Members' Personal Information would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the Personal Information of Plaintiff and the Class and all resulting damages.

123. Defendant owed Plaintiff and Class Members a duty to notify them within a reasonable time frame of any breach to its Personal Information. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiff and Class Members to take appropriate measures to protect its Personal Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of the Data Breach.

124. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals who Defendant knew or should have known would suffer injury-in-fact from its inadequate security protocols. After all, Defendant actively sought and obtained the Personal Information of Plaintiff and Class Members.

125. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Personal Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Personal Information;

b. Failing to comply with—and thus violating—FTCA, HIPAA and the applicable regulations;

c. Failing to adequately monitor the security of its networks and systems;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Personal Information;

f. Failing to detect in a timely manner that Class Members' Personal Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

126. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Personal Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial service industry. It was therefore foreseeable that the failure to adequately safeguard Class Members' Personal Information would result in one or more types of injuries to Class Members.

127. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' Personal Information. Defendant knew or should have known that its systems and technologies for processing and securing the Personal Information of Plaintiff and the Class had security vulnerabilities.

128. As a result of Defendant's negligence, the Personal Information and other sensitive information of Plaintiff and Class Members was compromised, placing them at a greater risk of identity theft and their Personal Information being disclosed to third parties without the consent of Plaintiff and the Class Members.

129. Simply put, Defendant's negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injuries-in-fact and damages. These injuries include, but are not limited to, the theft of their Personal Information by criminals, improper disclosure of their

Personal Information, lost benefit of their bargain, lost value of their Personal Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence. Moreover, injuries-in-fact and damages are ongoing, present and continuing.

130. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

131. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (1) strengthen its data security systems and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) continue to provide adequate credit monitoring to all Class Members for a period of ten years.

SECOND CAUSE OF ACTION
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

132. Plaintiff re-alleges and incorporates by reference paragraphs 1-111 of the Complaint as if fully set forth herein.

133. Under the Federal Trade Commission Act, Defendant had a duty to employ reasonable security measures. Specifically, this statute prohibits "unfair . . . practices in or affecting commerce," including (as interpreted and enforced by the FTC) the unfair practice of failing to use reasonable measures to protect confidential data.[14]

134. Moreover, Plaintiff's and Class Members' injuries are precisely the type of injuries that the FTCA guards against. After all, the FTC has pursued numerous enforcement actions against businesses that—because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the very same injuries that Defendant inflicted upon Plaintiff and Class Members.

135. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Personal Information.

[14] 15 U.S.C. § 45.

136. Defendant violated its duties and its obligations under HIPAA as a Business Associate by reason of the Data Breach.

THIRD CAUSE OF ACTION
Violations of the California Unfair Competition Law

California Civil Code §17200, *et seq*.

(On Behalf of Plaintiff and the Class)

137. Plaintiff re-alleges and incorporates by reference paragraphs 1-111 of the Complaint as if fully set forth herein.

138. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, et seq. ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

139. By reason of Defendant's above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiffs' and Class Members' Personal Information, Defendant engaged in unlawful, unfair and fraudulent business practices in violation of the UCL.

140. Plaintiff and Class Members suffered injury in fact and lost money or property as a result of Defendant's alleged violations of the UCL.

141. The acts, omissions, and conduct of Defendant as alleged herein constitute a "business practice" within the meaning of the UCL.

Unlawful Prong

142. Defendant's acts, omissions, and conduct violate the unlawful prong of the UCL. As alleged above, Defendant's failure to adequately and reasonably protect customer data by employing reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice, prohibited by section 5 of the FTCA.

143. Defendant's breach of section 5 of the FTCA also violates the unlawful prong of the UCL.

Unfair Prong

144. Defendant's acts, omissions, and conduct violate the unfair prong of the UCL because Defendants' acts, omissions, and conduct, as alleged herein, offended public policy and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and other Class Members. The gravity of Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests, other than Defendants' conduct described herein.

145. Defendant's failure to utilize, and to disclose that it does not utilize, industry standard security practices constitutes an unfair business practice under the UCL. Defendant's conduct is unethical, unscrupulous, and substantially injurious to the Class.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of all others similarly situated, requests the following relief:

A. An Order certifying this action as a class action and appointing Plaintiff as Class representatives, and the undersigned as Class Counsel;

B. A mandatory injunction directing Defendant to adequately safeguard the Personal Information of Plaintiff and the Class hereinafter by implementing improved security procedures and measures, including but not limited to an Order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete and purge the Personal Information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' Personal Information;

v. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

vi. prohibiting Defendant from maintaining Plaintiff's and Class Members' Personal Information on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

viii. requiring Defendant to conduct regular database scanning and securing checks;

ix. requiring Defendant to monitor ingress and egress of all network traffic;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Personal Information, as well as protecting the Personal Information of Plaintiff and Class Members;

xi. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xii. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor

Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;

xiii. appointing an independent and qualified cyber auditor to monitor Defendant's cyber hygiene, to be funded by Defendant; and

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

C. A mandatory injunction requiring that Defendant provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of Personal Information to unauthorized persons;

D. A mandatory injunction requiring Defendant to purchase credit monitoring and identity theft protection services for each Class Member for ten years;

E. An injunction enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen Personal Information;

F. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;

G. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

H. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

I. Granting the Plaintiff and the Class leave to amend this Complaint to conform to the evidence produced at trial;

J. For all other Orders, findings, and determinations identified and sought in this Complaint; and

K. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury for any and all issues in this action so triable as of right.

Dated: January 17, 2025

Respectfully Submitted,

/s/ Michael F. Ram

Michael F. Ram (SBN 104805)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Telephone: (415) 358-6913
Facsimile: (415) 358-6923
Email: mram@forthepeople.com

John A. Yanchunis*
JYanchunis@forthepeople.com
Ryan McGee*
rmcgee@forthepeople.com
Ronald Podolny*
ronald.podolny@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, FL 33602
T: (813) 223-5505
F: (813) 223-5402

**Pro hac vice forthcoming*

Counsel for Plaintiff and the Class